future internet

MDPI

Editorial

Cybersecurity in the IoT

Christos Tryfonopoulos * and Nicholas Kolokotronis

Department of Informatics and Telecommunications, University of the Peloponnese, GR 22100 Tripoli, Greece; nkolok@uop.gr
* Correspondence: trifon@uop.gr

The Internet of Things (IoT) has evolved into a vast ecosystem of massively interconnected devices delivering intelligent services across consumer, commercial, and industrial environments. Despite its transformative potential, the IoT remains inherently vulnerable. Many deployed devices are resource-constrained and frequently designed without robust security primitives, often lacking strong authentication, secure update mechanisms, or proper credential management. The integration of IoT infrastructures with cloud platforms and distributed services further increases architectural complexity, reduces visibility, and expands the attack surface. Modern botnets increasingly weaponize both IoT devices and cloud resources, while supply chain compromises and zero-trust violations expose systemic weaknesses in traditionally perimeter-based security models. In this context, intelligent, adaptive, and cross-layer security approaches are no longer optional but essential for effective preparation, prevention, detection, and mitigation of cyber-threats.

This Special Issue aims at presenting state-of-the-art methodologies, algorithms, analyses, protocols, and frameworks that address cybersecurity challenges in IoT ecosystems. The accepted contributions reflect the breadth of the original call, covering AI-driven security techniques, architectural and protocol-level innovations, domain-specific cybersecurity analyses, and disruptive defensive mechanisms spanning device, network, and cloud-integrated environments. To present a coherent perspective on the field's evolution, the accepted papers are organized into three thematic groups. The first group establishes the threat landscape and formal foundations of IoT security through surveys, systematization efforts, and domain-specific analyses. The second group focuses on AI-based intrusion and anomaly detection mechanisms that enable intelligent and adaptive defense in large-scale IoT and cyber–physical systems, while the third group of papers highlights secure-by-design architectures, lightweight cryptographic protocols, and privacy-preserving mechanisms that embed security directly into IoT infrastructures. This grouping reflects a logical research trajectory—from understanding vulnerabilities to detecting adversarial behavior and engineering resilient and trustworthy IoT systems—thereby capturing the multidimensional nature of cybersecurity in the Future Internet.

The first group of contributions establishes the conceptual and analytical foundations of IoT cybersecurity by systematizing knowledge, formalizing security notions, and examining domain-specific threat landscapes. The survey [1] provides a general yet comprehensive overview of vulnerabilities, architectural weaknesses, and mitigation strategies across the IoT ecosystem, offering a holistic synthesis of device, network, and data-layer security challenges. Complementing this broad perspective, the work in [2] delivers a knowledge systematization on delegated security in IoT, introducing formalized security notions and a mathematical interpretation of the confidentiality/integrity/availability triad within constrained environments. By analyzing delegation as a design paradigm, this work strengthens the theoretical underpinnings of resource-aware IoT protection. At the

Received: 27 February 2026
Accepted: 28 February 2026
Published: 2 March 2026

domain level, the authors in [3] focus on healthcare IoT, presenting a layered taxonomy of threats across perception, network, and application layers while emphasizing regulatory and privacy implications in safety-critical environments. Finally, the work in [4] extends the discussion to Unmanned Aerial Vehicle (UAV) ecosystems, examining drone-specific threat models, forensic artifacts, and persistent operational challenges. Together, these works map the evolving attack surface of IoT systems, highlight the need for domain-aware threat modeling and formal reasoning, and define the risk landscape that motivates the technical innovations presented in the rest of the contributions of this Special Issue.

The second group reflects the growing centrality of artificial intelligence in defending IoT infrastructures. These contributions collectively explore supervised, unsupervised, and hybrid learning paradigms for intrusion detection and anomaly identification in dynamic and heterogeneous environments. The work in [5] evaluates multiple machine learning and deep learning classifiers for DDoS discrimination, emphasizing the importance of feature selection and preprocessing for performance optimization, while [6] advances deep intrusion detection architectures by integrating residual temporal convolutional modules with attention mechanisms; this allows for improved feature extraction and generalization capability across benchmark datasets. Moving toward reduced reliance on labeled data, refs. [7,8] adopt semi-supervised and unsupervised paradigms centered on autoencoder-based feature extraction. The work in [7] proposes a hybrid framework combining basic and deep autoencoders with one-class classification and density-based clustering, enabling detection of previously unseen attacks while addressing data imbalance. Similarly, the authors in [8] apply a GRU-enhanced stacked autoencoder in smart grid environments, coupling deep representation learning with anomaly detection algorithms to secure cyber–physical energy infrastructures. Collectively, this group of contributions illustrates a methodological shift toward adaptive, data-driven security intelligence capable of addressing the scale, heterogeneity, and evolving attack patterns of modern IoT deployments via AI-driven approaches.

While detection is critical, proactive security engineering remains relevant; the third group of works presents constructive approaches that embed security and privacy directly into IoT architectures, protocols, and communication layers. The work in [9] introduces a secure and auditable registry architectural pattern based on message-oriented middleware, emphasizing reusability, real-world applicability, and integration into broader security pattern languages. This contribution highlights the importance of auditability and accountability in large-scale IoT systems transitioning from legacy infrastructures. At the protocol level, the authors of [10] propose a lightweight authenticated one-pass key establishment mechanism implemented on a micro-controller with Reduced Instruction Set Computing (RISC-V) architecture. By combining elliptic curve cryptographic schemes and optimizing for constrained devices, the work demonstrates how strong security guarantees can be achieved with minimal computational overhead. Complementing these architectural and cryptographic contributions, the work in [11] addresses privacy risks emerging from next-generation Wi-Fi sensing capabilities. By modeling channel contention and introducing conservative interference injection as a defense strategy, it provides a physical-layer privacy-preserving mechanism that balances sensing degradation with bandwidth efficiency. Altogether, this group of papers emphasizes that IoT cybersecurity must be engineered across layers—from hardware and cryptography to middleware and wireless communication.

Taken together, the contributions in this Special Issue outline a coherent research trajectory for cybersecurity in the IoT era. Initially, a rigorous understanding of the threat landscape and formal security foundations to characterize vulnerabilities across diverse and domain-specific IoT ecosystems is provided via the works in [1–4]. As IoT environ-

ments grow in scale and complexity, adaptive and intelligent detection mechanisms [5–8] that leverage machine/deep learning focus on identifying evolving attack patterns in real time. Finally, secure-by-design architectures, lightweight cryptographic protocols, and privacy-preserving mechanisms shift the focus from reactive detection to embedding IoT cybersecurity at the system level via hardware validation and physical-layer privacy defenses. This progression, from understanding risk to detecting adversarial behavior and engineering resilient systems, captures the multidimensional nature of IoT security and highlights the maturing of the research field: moving beyond isolated solutions towards integrated, cross-layer, and intelligence-driven approaches capable of securing the Future Internet.

Author Contributions: All authors contributed equally to this editorial. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Dritsas, E.; Trigka, M. A Survey on Cybersecurity in IoT. *Future Internet* **2025**, *17*, 30. [CrossRef]
2. Geloczi, E.; Klement, F.; Struck, P.; Katzenbeisser, S. SoK: Delegated Security in the Internet of Things. *Future Internet* **2025**, *17*, 202. [CrossRef]
3. Madanian, S.; Chinbat, T.; Subasinghage, M.; Airehrour, D.; Hassandoust, F.; Yongchareon, S. Health IoT Threats: Survey of Risks and Vulnerabilities. *Future Internet* **2024**, *16*, 389. [CrossRef]
4. Adel, A.; Jan, T. Watch the Skies: A Study on Drone Attack Vectors, Forensic Approaches, and Persisting Security Challenges. *Future Internet* **2024**, *16*, 250. [CrossRef]
5. Alenezi, M.N. Significance of Machine Learning-Driven Algorithms for Effective Discrimination of DDoS Traffic Within IoT Systems. *Future Internet* **2025**, *17*, 266. [CrossRef]
6. Cui, B.; Chai, Y.; Yang, Z.; Li, K. Intrusion Detection in IoT Using Deep Residual Networks with Attention Mechanisms. *Future Internet* **2024**, *16*, 255. [CrossRef]
7. Kaliyaperumal, P.; Periyasamy, S.; Thirumalaisamy, M.; Balusamy, B.; Benedetto, F. A Novel Hybrid Unsupervised Learning Approach for Enhanced Cybersecurity in the IoT. *Future Internet* **2024**, *16*, 253. [CrossRef]
8. Harrou, F.; Bouyeddou, B.; Dairi, A.; Sun, Y. Exploiting Autoencoder-Based Anomaly Detection to Enhance Cybersecurity in Power Grids. *Future Internet* **2024**, *16*, 184. [CrossRef]
9. Maña, A.; Jaime, F.J.; Gutiérrez, L. A Secure Auditable Remote Registry Pattern for IoT Systems. *Future Internet* **2024**, *16*, 405. [CrossRef]
10. Dang, T.K.; Nguyen, K.D.; Kieu-Do-Nguyen, B.; Hoang, T.T.; Pham, C.K. Realization of Authenticated One-Pass Key Establishment on RISC-V Micro-Controller for IoT Applications. *Future Internet* **2024**, *16*, 157. [CrossRef]
11. Sharma, A.; Wang, H.; Mishra, D.; Seneviratne, A. Conservative Interference Injection to Minimize Wi-Fi Sensing Privacy Risks and Bandwidth Loss. *Future Internet* **2025**, *17*, 20. [CrossRef]